TRANSMITTAL FORM	Attorney Docket No. RPS920010190US1/2370P

In re the application of: **Philip Lee CHILDS et al.** Confirmation No: **7874**

Serial No: **10/063,402** Group Art Unit: **2145**

Filed: **April 18, 2002** Examiner: **Bhatia, Ajay M.**

For: **Autonomic System for Selective Administration Isolation of a Secure Remote Management of Systems in a Computer Network**

ENCLOSURES *(check all that apply)*		
☐ Amendment/Reply	☐ Assignment and Recordation Cover Sheet	☐ After Allowance Communication to Group
☐ After Final	☐ Part B-Issue Fee Transmittal	☐ Notice of Appeal
☐ Information disclosure statement	☐ Letter to Draftsman	■ Appeal Brief
☐ Form 1449	☐ Drawings	☐ Status Letter
☐ (X) Copies of References	☐ Petition	■ Postcard
■ Extension of Time Request *	☐ Fee Address Indication Form	☐ Other Enclosure(s) *(please identify below):*
☐ Express Abandonment	☐ Terminal Disclaimer	
☐ Certified Copy of Priority Doc	☐ Power of Attorney and Revocation of Prior Powers	03/29/2006 MBIZUNES 00000073 10063402
☐ Response to Incomplete Appln	☐ Change of Correspondence Address	01 FC:1252 450.00 OP
☐ Response to Missing Parts	***Extension of Term: Pursuant to 37 CFR 1.136, Applicant petitions the Commissioner to extend the time for response for two month(s), from February 1, 2006 to April 1, 2006.**	
☐ Executed Declaration by Inventor(s)		

CLAIMS

FOR	Claims Remaining After Amendment	Highest # of Claims Previously Paid For	Extra Claims	RATE	FEE
Total Claims	12	21	0	$ 50.00	$ 0.00
Independent Claims	3	4	0	$200.00	$ 0.00
				Total Fees	$ 0.00

METHOD OF PAYMENT

■	Check no. 10201 in the amount of **$450.00** is enclosed for payment of extension fees.
■	Charge **$500.00** to Deposit Account No. 50-3533 (Lenovo, Inc.) for payment of appeal fee.
■	Charge any additional fees or credit any overpayment to Deposit Account No. 50-3533 (Lenovo, Inc.).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Attorney Name	Kelvin M. Vivian, Reg. No. 53,727
Signature	
Date	March 17, 2006

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on **March 17, 2006**.

Type or printed name	Jinny Nguyen
Signature	

OIPE IAP86 MAR 29 2006 PATENT & TRADEMARK OFFICE

Attorney Docket: RPS920010190US1/2370P

CERTIFICATE OF MAIL

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on **March 17, 2006**.

Jimmy Nguyen

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of: Philip Lee CHILDS et al.

Serial No: 10/063,402

Filed: April 18, 2002

Date: March 17, 2006

Confirmation No: 7874

Group Art Unit: 2145

Examiner: Bhatia, Ajay M.

Title: AUTONOMIC SYSTEM FOR SELECTIVE ADMINISTRATION ISOLATION OF A SECURE REMOTE MANAGEMENT OF SYSTEMS IN A COMPUTER NETWORK

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

(1) Real Party in Interest

The real party in interest is Lenovo Incorporated.

(2) Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

(3) Status of Claims

Claims 5-14 and 19-20 are pending in the present application.

03/29/2006 MBIZUNES 00000074 10063402
01 FC:1402 500.00 DA

Claims 5-7, 9-13, and 19-20 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,968,177 to Batten-Carew et al. ("Batten-Carew").

Claim 8 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Batten-Carew in view of U.S. Patent No. 6,181,803 to Davis ("Davis").

Claims 5-14, 19 and 20 are being appealed.

(4) Status of Amendments

There are no unentered amendments.

(5) Summary of Claimed Subject Matter

Independent claim 5 recites a method for autonomic administration isolation for a secure remote management in a computer network. The method includes isolating administrative access to a plurality of client systems in a computer network via a data center. Specification, paragraph 0009; FIG 1. The method further includes utilizing the data center to control remote initiation of services in the plurality of client systems by an administrator system. Specification, paragraph 0012; FIG 1. The administrator system is a computer through which an administrator manages at least one of the plurality of client systems. Specification, paragraph 0009; FIG 1.

As further recited in claim 5, utilizing the data center further includes: verifying authentication of the administrator system by the data center, receiving a service command from the authenticated administrator system in the data center, determining in the data center whether the authenticated administrator system has authorization to perform the service command in the at least one managed client system, and issuing a trusted message from the data center to the at least one managed client system when the

authenticated administrator system does have authorization to perform the service command. Specification, paragraphs 0009-0011; FIG 2.

Independent claim 7 recites an autonomic system for selective administration isolation for secure remote management in a computer network that, in essence, implements the method of claim 5.

Independent claim 19 recites a computer readable medium containing program instructions for autonomic administration isolation in a computer network for a secure remote management that, in essence, implements the method of claim 5.

(6) Grounds of Rejection to be Reviewed on Appeal

1. Appellant requests review as to claims 5-7, 9-13, and 19-20 and their rejection under 35 U.S.C. § 102(b) as being anticipated by Batten-Carew.

2. Appellant requests review as to claim 8 and its rejection under 35 U.S.C. § 103(a) as being unpatentable over Batten-Carew in view of Davis.

(7) Argument

1. Claims 5-7, 9-13, and 19-20 are not properly rejected under 35 U.S.C. § 102(b) as being anticipated by Batten-Carew.

Claim 5 recites a method for autonomic administration isolation. The method includes isolating administrative access to a plurality of client systems in a computer system via a data network. The method also includes issuing a trusted message from a data center to the at least one managed client system when the authenticated administrator system does have authorization to perform the service command.

A potential advantage of such a method is that system administrators never have direct access to a client's operating system log-ons or security credentials (specification paragraph 0011).

Batten-Carew fails to disclose several aspects of claim 5.

A. Batten-Carew Fails to Disclose Isolating Administrative Access to a Plurality of Client Systems in a Computer Network via a Data Center

Batten-Carew discloses a secure communication system including an administrative entity, a serving entity, and one or more end-users (col. 2, ll. 62-66; FIG. 1). In operation, when the administrative entity has an administrative function to perform on an end-user, the administrative entity sends an administrative function request to the serving entity (col. 4, ll. 22-25). The serving entity verifies the identity of the administrative entity and verifies whether the administrative entity is authorized to perform the administrative function request (col. 4 line 58 - col. 5 line 5). If the administrative request is consistent, then the administrative request is provided directly to the end-user or back to the administrative entity (which will then provide the information to the end-user) (col. 7 ll. 8-15).

While Batten-Carew discloses that the serving entity can provide an administrative request (from an administrative entity) directly to an end-user, Batten-Carew also discloses that (in the same embodiment) the administrative request can also be provided back to the administrative entity, which will subsequently provide the information to the end-user (col. 7, ll. 13-15). Accordingly, Batten-Carew fails to

disclose isolating administrative access to a plurality of client systems in a computer network via a data center, as required by claim 5.

In the Advisory Action dated November 18, 2005, the Examiner cites column 3, lines 15-25 of Batten-Carew as disclosing isolating administrative access to a plurality of client systems in a computer network via a data center. The Appellant respectfully disagrees. In the cited portion, Batten-Carew discloses only the end-users being in (3) separate groups to signify that each group of end-users may be located at separate locales (col. 3, ll. 21-23). Such a disclosure does not disclose isolating administrative access to a plurality of client systems in a computer network via a data center, as recited in claim 5.

B. Batten-Carew Fails to Disclose Issuing a Trusted Message from the Data Center to at least One Managed Client when the Authenticated Administrative Does Have Authorization to Perform the Service Command

In rejecting claim 5, the Examiner cites several portions of Batten-Carew – specifically, col. 4 lines 45-57, col. 6 lines 9-22, col. 7 lines 30-34, col. 7. 35-48, and col. 7 line 65 – col. 8 line 14 - as disclosing issuing a trusted message from the data center to at least one managed client when the authenticated administrative system has permission to perform a service command. The Appellant respectfully disagrees.

In the cited portions, Batten-Carew discloses only the serving entity verifying a signature of the administrative entity, and the administrative entity verifying a signature of the serving entity. While Batten-Carew may disclose verifying authentication of the administrative system ("administrative entity") by the data center ("serving entity"), Batten-Carew clearly does not disclose issuing a trusted message from the data center to

at least one managed client system when the authenticated administrator system does have authorization to perform the service command (emphasis added).

Instead, (as discussed above) in Batten-Carew's system, if the serving entity verifies an administrative request of an administrative entity, the administrative request is either provided *directly to* an end-user, or the administrative request is returned to the administrative entity (which will subsequently provide the information to the user) (col. 7, ll. 9-15). There is no mention in Batten-Carew of the serving entity ("data center") issuing a trusted message directly to an end-user ("managed client system"). Nor is it inherent that the serving entity provides a trusted message to an end-user. *See* MPEP 2163.07 - "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

In the Advisory Action, the Examiner asserts that the Applicant does not define the term "trusted message" and, therefore, the Examiner must give the term the broadest possible interpretation of one of skill in the art at the time of the invention. Although the Examiner is entitled to a reasonably broad interpretation of the claim terms, the Examiner must interpret the claims consistent with the specification. MPEP §2111, citing *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969). Paragraph 0011 of the Applicant's specification discloses that a trusted message is a message that is encrypted and has an associated signature.

In the Advisory Action, the Examiner further asserts that Batten-Carew discloses a public key system in column3, line 15. While Batten-Carew does disclose a public key system, the public key system is used only to permit the end-users to securely communicate amongst one another, because (as stated above), each of the groups of end-users may be in physically separate locales (col. 14-23). Batten-Carew fails to disclose that the public key system is used for communication between a serving entity ("data center") and an end-user ("managed client system").

C. The Examiner has not met the basic criteria to establish anticipation

To anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

As discussed above, Batten-Carew fails to disclose isolating administrative access to a plurality of client systems in a computer network via a data center. Batten-Carew also fails to disclose issuing a trusted message from the data center to at least one managed client system when the authenticated administrator system does have authorization to perform the service command, as required by claim 5. Appellant respectfully submits, therefore, Batten-Carew does not anticipate claim 5. Thus, claim 5 is improperly rejected under § 102(b). Claim 6 depends from claim 5 and, therefore, is

improperly rejected for at least the same reasons. Claims 7 and 19 each recites features corresponding to those of claim 5 and, therefore, are also improperly rejected for at least the same reasons. Claims 9-14 and 20 respectively depend directly or indirectly from claims 7 and 19 and, therefore, are improperly rejected for at least the same reasons.

2. Claim 8 is not properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Batten-Carew in view of Davis.

Claim 8 depends from claim 7, and further recites the at least one administrator system includes authentication capabilities via an embedded security chip for unique system identification and biometric identification for unique user identification (see Specification, paragraph 0010).

A. Davis Fails to Disclose Isolating Administrative Access to a Plurality of Client Systems in a Computer Network via a Data Center

Putting aside the issue of whether Davis discloses the limitations of claim 8, Davis (as with Batten-Carew) fails to disclose isolating administrative access to a plurality of client systems in a computer network via a data center. Davis also fails to disclose issuing a trusted message from the data center to at least one managed client system when the authenticated administrator system does have authorization to perform the service command. The appellant respectfully submits that claim 8 is improperly rejected for at least reasons similar to those discussed above.

B. The Examiner has not met the basic criteria required to establish a prima facie *case of obviousness*

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Both Batten-Carew and Davis fail to disclose isolating administrative access to a plurality of client systems in a computer network via a data center. Batten-Carew and Davis also fail to disclose issuing a trusted message from the data center to at least one managed client system when the authenticated administrator system does have authorization to perform the service command. Consequently, the combination of Batten-Carew and Davis cannot render claim 5 obvious, and the Examiner has not made a *prima facie* showing of obviousness.

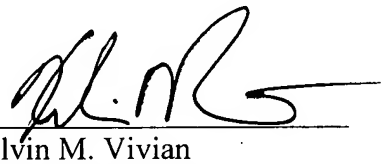
Conclusion

Neither Batten-Carew and Davis discloses isolating administrative access to a plurality of client systems in a computer network via a data center. Batten-Carew and Davis also fail to disclose issuing a trusted message from the data center to at least one managed client system when the authenticated administrator system does have authorization to perform the service command, as required by the claims. The appellant, therefore, respectfully submits that the pending claims 5-14 and 19-20 are not properly rejected under § 102 or § 103.

Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 50-3533 (Lenovo, Inc.).

Respectfully submitted,

SAWYER LAW GROUP LLP



March 17, 2006
Date

Kelvin M. Vivian
Attorney for Applicant
Reg. No. 53,727
(650) 493-4540

Appendix of Claims

1-4. (Cancelled)

5. (Previously Presented) A method for autonomic administration isolation for a secure remote management in a computer network, the method comprising:

(a) isolating administrative access to a plurality of client systems in a computer network via a data center; and

(b) utilizing the data center to control remote initiation of services in the plurality of client systems by an administrator system, the administrator system being a computer through which an administrator manages at least one of the plurality of client systems, wherein utilizing the data center further includes,

(b1) verifying authentication of the administrator system by the data center;

(b2) receiving a service command from the authenticated administrator system in the data center;

(b3) determining in the data center whether the authenticated administrator system has authorization to perform the service command in the at least one managed client system; and

(b4) issuing a trusted message from the data center to the at least one managed client system when the authenticated administrator system does have authorization to perform the service command.

6. (Previously Presented) The method of claim 5, further comprising (c) validating and decrypting the trusted message in the at least one managed client system to perform the service command.

7. (Previously Presented) An autonomic system for selective administration isolation for secure remote management in a computer network, the system comprising:

a network;

at least one administrator system coupled to the network, the at least one administrator system operable to transmit one or more service commands for managing one or more client systems;

at least one client system coupled to the network; and

a data center coupled to the at least one administrator system and to the at least one client system via the network, the data center for:

isolating administrative access to the at least one client system and controlling remote initiation of services in the at least one client system by the at least one administrator system including,

receiving a service command from the at least one administrator system, the service command having been issued after authentication of a first user associated with the at least one administrator system; and

issuing a trusted message to remotely control the at least one client system according to the service command, the trusted message having been issued after authentication of a second user associated with the data center, wherein the first user is different from the second user.

8. (Original) The system of claim 7, wherein the at least one administrator system includes authentication capabilities via an embedded security chip for unique system identification and biometric identification for unique user identification.

9. (Previously Presented) The system of claim 7, wherein the data center verifies authentication of the at least one administrator system.

10. (Previously Presented) The system of claim 7, wherein the authentication of a second user associated with the data center includes a user ID and password known only to the data center and an agent running on the at least one client system.

11. (Previously Presented) The system of claim 9, wherein the data center determines whether the authenticated administrator system has authorization to perform the service command in the at least one client system prior to issuing the trusted message to the at least one client system.

12. (Previously Presented) The system of claim 11, wherein the data center issues a trusted message to the at least one client system when the authenticated administrator system does have authorization to perform the service command.

13. (Previously Presented) The system of claim 12, wherein the at least one client system validates and decrypts the trusted message to perform the service command.

14. (Original) The system of claim 9, wherein the network further comprises a world wide web network.

15-18. (Cancelled)

19. (Previously Presented) A computer readable medium containing program instructions tangibly stored thereon for autonomic administration isolation in a computer network for a secure remote management, the program instructions for:

(a) isolating administrative access to a plurality of client systems in a computer network via a data center; and

(b) controlling remote initiation of services in the plurality of client systems by an administrator system via the data center, the administrator system being a computer through which an administrator manages at least one of the plurality of client systems, wherein controlling remote initiation of services via the data center includes,

(b1) verifying authentication of the administrator system by the data center;

(b2) receiving a service command from the authenticated administrator system in the data center;

(b3) determining in the data center whether the authenticated administrator system has authorization to perform the service command in the at least one managed client system; and

(b4) issuing a trusted message from the data center to the at least one managed client system when the authenticated administrator system does have authorization to perform the service command.

20. (Previously Presented) The computer readable medium of claim 19, further comprising (c) validating and decrypting the trusted message in the at least one managed client system to perform the service command.

21-23. (Cancelled)